

Amendments to the Claims

- 1 Claim 1 (currently amended): A computer program product for providing end-to-end user
2 authentication for legacy host application access, said computer program product embodied on a
3 computer-readable medium readable by a computing device in a computing environment and
4 comprising:
- 5 computer-readable program code means for establishing a secure session from a client
6 machine to a server machine using a digital certificate transmitted from said client machine to said
7 server machine, wherein said digital certificate represents representing said client machine or a
8 user thereof;
- 9 computer-readable program code means for storing said transmitted digital certificate at
10 said server machine;
- 11 computer-readable program code means for establishing a session from said server
12 machine to a host system on behalf of said client machine, responsive to establishment of said
13 secure session, using a legacy host communication protocol;
- 14 computer-readable program code means for passing said stored digital certificate from
15 said server machine to a host access security system, responsive to receiving, at said server
16 machine, a request from said host system for log-on information of said user;
- 17 computer-readable program code means, operable in said host access security system, for
18 using said passed digital certificate to locate access credentials for said user;
- 19 computer-readable program code means for returning, from said host access security

20 system to said server machine, a user identifier associated with said located access credentials and
21 either accessing a stored password or a generated password substitute representing said located
22 credentials; and

23 computer-readable program code means for using forwarding said stored returned user
24 identifier and password or said-generated password substitute from said server machine to said
25 host system as a response to said request for log-on information, such that said forwarded user
26 identifier and password or password substitute can be used by said host system to transparently
27 log said user on to a secure legacy host application executing at said host system, without
28 requiring change to said host system.

1 Claim 2 (original): The computer program product as claimed in Claim 1, wherein said digital
2 certificate is an X.509 certificate.

1 Claim 3 (currently amended): The computer program product as claimed in Claim 1 or Claim 2,
2 wherein said communication protocol is a 3270 emulation protocol.

1 Claim 4 (currently amended): The computer program product as claimed in Claim 1 or Claim 2,
2 wherein said communication protocol is a 5250 emulation protocol.

1 Claim 5 (currently amended): The computer program product as claimed in Claim 1 or Claim 2,
2 wherein said communication protocol is a Virtual Terminal protocol.

1 Claim 6 (original): The computer program product as claimed in Claim 3, wherein said host
2 access security system is a Resource Access Control Facility (RACF) system.

1 Claim 7 (original): The computer program product as claimed in Claim 1, wherein said server
2 machine is a Web application server machine.

1 Claim 8 (currently amended): A computer program product for providing end-to-end user
2 authentication for legacy host application access, said computer program product embodied on a
3 computer-readable medium readable by a computing device in a computing environment and the
4 computer program product as claimed in Claim 1, further comprising:

5 computer-readable program code means for establishing a secure session from a client
6 machine to a server machine using a digital certificate transmitted from said client machine to said
7 server machine, wherein said digital certificate represents said client machine or a user thereof;

8 computer-readable program code means for storing said transmitted digital certificate at
9 said server machine;

10 computer-readable program code means for establishing a session from said server
11 machine to a host system on behalf of said client machine, responsive to establishment of said
12 secure session, using a legacy host communication protocol;

13 computer-readable program code means for automatically sending a log-on message from
14 said client machine to said server machine, responsive to receiving, at said client machine, a

15 request from said host system for log-on information of said user, wherein said log-on message
16 uses placeholder syntax in place of a user identifier and a password of said user;

17 computer-readable program code means for passing said stored digital certificate from
18 said server machine to a host access security system, responsive to receiving, at said server
19 machine, said log-on message from said client machine;

20 computer-readable program code means, operable in said host access security system, for
21 using said passed digital certificate to locate access credentials for said user;

22 computer-readable program code means for returning, from said host access security
23 system to said server machine, a user identifier associated with said located access credentials and
24 either a stored password or a generated password substitute representing said located credentials;

25 computer-readable program code means for modifying, by said server machine, said
26 received log-on message by replacing said placeholder syntax with said returned user identifier
27 and password or password substitute; and

28 computer-readable program code means for forwarding said modified log-on message
29 from said server to said host system as a response to said request for log-on information, such
30 that said user identifier and password or password substitute from said forwarded log-on message
31 can be used by said host system to transparently log said user on to a secure legacy host
32 application executing at said host system, without requiring change to said host system.

33 computer-readable program code means for requesting by said legacy host application,
34 responsive to said computer-readable program code means for establishing said session, log-on
35 information for said user;

36 ~~computer-readable program code means for responding to said request for log on~~
37 ~~information by sending a log on message with placeholders from said client machine to said server~~
38 ~~machine, said placeholders representing a user identification and a password of said user; and~~
39 ~~computer-readable program code means for substituting a user identifier associated with~~
40 ~~said located access credentials and said stored password or said generated passticket for said~~
41 ~~placeholders in said log on message.~~

Claim 9 (canceled)

1 Claim 10 (currently amended): A system for providing end-to-end user authentication for legacy
2 host application access in a computing environment, comprising:

3 means for establishing a secure session from a client machine to a server machine using a
4 digital certificate transmitted from said client machine to said server machine, wherein said digital
5 certificate represents representing said client machine or a user thereof;

6 means for storing said transmitted digital certificate at said server machine;

7 means for establishing a session from said server machine to a host system on behalf of
8 said client machine, responsive to establishment of said secure session, using a legacy host
9 communication protocol;

10 means for passing said stored digital certificate from said server machine to a host access
11 security system, responsive to receiving, at said server machine, a request from said host system
12 for log-on information of said user;

Serial No. 09/466,625

-6-

Docket RSW990077

13 means, operable in said host access security system, for using said passed digital certificate
14 to locate access credentials for said user;

15 means for returning, from said host access security system to said server machine, a user
16 identifier associated with said located access credentials and either accessing a stored password or
17 a generated password substitute representing said located credentials; and

18 means for using forwarding said stored returned user identifier and password or said
19 generated password substitute from said server machine to said host system as a response to said
20 request for log-on information, such that said forwarded user identifier and password or password
21 substitute can be used by said host system to transparently log said user on to a secure legacy host
22 application executing at said host system, without requiring change to said host system.

1 Claim 11 (original): The system as claimed in Claim 10, wherein said digital certificate is an
2 X.509 certificate.

1 Claim 12 (currently amended): The system as claimed in Claim 10 ~~or Claim 11~~, wherein said
2 communication protocol is a 3270 emulation protocol.

1 Claim 13 (currently amended): The system as claimed in Claim 10 ~~or Claim 11~~, wherein said
2 communication protocol is a 5250 emulation protocol.

1 Claim 14 (currently amended): The system as claimed in Claim 10 ~~or Claim 11~~, wherein said

2 communication protocol is a Virtual Terminal protocol.

1 Claim 15 (original): The system as claimed in Claim 12, wherein said host access security system
2 is a Resource Access Control Facility (RACF) system.

1 Claim 16 (original): The system as claimed in Claim 10, wherein said server machine is a Web
2 application server machine.

1 Claim 17 (currently amended): A system for providing end-to-end user authentication for legacy
2 host application access in a computing environment. ~~The system as claimed in Claim 10, further~~
3 comprising:

4 means for establishing a secure session from a client machine to a server machine using a
5 digital certificate transmitted from said client machine to said server machine, wherein said digital
6 certificate represents said client machine or a user thereof;

7 means for storing said transmitted digital certificate at said server machine;

8 means for establishing a session from said server machine to a host system on behalf of
9 said client machine, responsive to establishment of said secure session, using a legacy host
10 communication protocol;

11 means for automatically sending a log-on message from said client machine to said server
12 machine, responsive to receiving, at said client machine, a request from said host system for log-
13 on information of said user, wherein said log-on message uses placeholder syntax in place of a

14 user identifier and a password of said user;

15 means for passing said stored digital certificate from said server machine to a host access
16 security system, responsive to receiving, at said server machine, said log-on message from said
17 client machine;

18 means, operable in said host access security system, for using said passed digital certificate
19 to locate access credentials for said user;

20 means for returning, from said host access security system to said server machine, a user
21 identifier associated with said located access credentials and either a stored password or a
22 generated password substitute representing said located credentials;

23 means for modifying, by said server machine, said received log-on message by replacing
24 said placeholder syntax with said returned user identifier and password or password substitute;
25 and

26 means for forwarding said modified log-on message from said server to said host system
27 as a response to said request for log-on information, such that said user identifier and password or
28 password substitute from said forwarded log-on message can be used by said host system to
29 transparently log said user on to a secure legacy host application executing at said host system,
30 without requiring change to said host system.

31 means for requesting by said legacy host application, responsive to said means for
32 establishing said session, log-on information for said user;

33 means for responding to said request for log on information by sending a log on message
34 with placeholders from said client machine to said server machine, said placeholders representing

35 ~~a user identification and a password of said user, and~~
36 ~~means for substituting a user identifier associated with said located access credentials and~~
37 ~~said stored password or said generated passticket for said placeholders in said log on message.~~

Claim 18 (canceled)

1 Claim 19 (currently amended): A method for providing end-to-end user authentication for legacy
2 host application access in a computing environment, comprising the steps of:

3 establishing a secure session from a client machine to a server machine using a digital

4 certificate transmitted from said client machine to said server machine, wherein said digital

5 certificate represents representing said client machine or a user thereof;

6 storing said transmitted digital certificate at said server machine;

7 establishing a session from said server machine to a host system on behalf of said client
8 machine, responsive to establishment of said secure session, using a legacy host communication
9 protocol;

10 passing said stored digital certificate from said server machine to a host access security
11 system, responsive to receiving, at said server machine, a request from said host system for log-on
12 information of said user;

13 using, by said host access security system, said passed digital certificate to locate access
14 credentials for said user;

15 returning, from said host access security system to said server machine, a user identifier

Serial No. 09/466,625

-10-

Docket RSW990077

16 associated with said located access credentials and either accessing a stored password or a
17 generated password substitute representing said located credentials; and
18 forwarding using said stored returned user identifier and password or said-generated
19 password substitute from said server machine to said host system as a response to said request for
20 log-on information, such that said forwarded user identifier and password or password substitute
21 can be used by said host system to transparently log said user on to a secure legacy host
22 application executing at said host system, without requiring change to said host system.

1 Claim 20 (original): The method as claimed in Claim 19, wherein said digital certificate is an
2 X.509 certificate.

1 Claim 21 (currently amended): The method as claimed in Claim 19 or ~~Claim 20~~, wherein said
2 communication protocol is a 3270 emulation protocol.

1 Claim 22 (currently amended): The method as claimed in Claim 19 or ~~Claim 20~~, wherein said
2 communication protocol is a 5250 emulation protocol.

1 Claim 23 (currently amended): The method as claimed in Claim 19 or ~~Claim 20~~, wherein said
2 communication protocol is a Virtual Terminal protocol.

1 Claim 24 (original): The method as claimed in Claim 21, wherein said host access security system

2 is a Resource Access Control Facility (RACF) system.

1 Claim 25 (original): The method as claimed in Claim 19, wherein said server machine is a Web
2 application server machine.

1 Claim 26 (currently amended): A method for providing end-to-end user authentication for legacy
2 host application access in a computing environment. The method as claimed in Claim 19, further
3 comprising the steps of:

4 establishing a secure session from a client machine to a server machine using a digital
5 certificate transmitted from said client machine to said server machine, wherein said digital
6 certificate represents said client machine or a user thereof;

7 storing said transmitted digital certificate at said server machine;

8 establishing a session from said server machine to a host system on behalf of said client
9 machine, responsive to establishment of said secure session, using a legacy host communication
10 protocol;

11 automatically sending a log-on message from said client machine to said server machine,
12 responsive to receiving, at said client machine, a request from said host system for log-on
13 information of said user, wherein said log-on message uses placeholder syntax in place of a user
14 identifier and a password of said user;

15 passing said stored digital certificate from said server machine to a host access security
16 system, responsive to receiving, at said server machine, said log-on message from said client

17 machine;

18 using, by said host access security system, said passed digital certificate to locate access
19 credentials for said user;

20 returning, from said host access security system to said server machine, a user identifier
21 associated with said located access credentials and either a stored password or a generated
22 password substitute representing said located credentials;

23 modifying, by said server machine, said received log-on message by replacing said
24 placeholder syntax with said returned user identifier and password or password substitute; and

25 forwarding said modified log-on message from said server to said host system as a
26 response to said request for log-on information, such that said user identifier and password or
27 password substitute from said forwarded log-on message can be used by said host system to
28 transparently log said user on to a secure legacy host application executing at said host system,
29 without requiring change to said host system.

30 requesting by said legacy host application, responsive to said step of establishing said
31 session, log on information for said user;

32 ~~responding to said request for log on information by sending a log on message with~~
33 ~~placeholders from said client machine to said server machine, said placeholders representing a~~
34 ~~user identification and a password of said user; and~~

35 ~~substituting a user identifier associated with said located access credentials and said stored~~
36 ~~password or said generated passticket for said placeholders in said log on message.~~

Claim 27 (canceled)

1 Claim 28 (new): The method as claimed in Claim 26, wherein said digital certificate is an X.509
2 certificate.

1 Claim 29 (new): The method as claimed in Claim 26, wherein said communication protocol is a
2 3270 emulation protocol.

1 Claim 30 (new): The method as claimed in Claim 26, wherein said communication protocol is a
2 5250 emulation protocol.

1 Claim 31 (new): The method as claimed in Claim 26, wherein said communication protocol is a
2 Virtual Terminal protocol.

1 Claim 32 (new): The method as claimed in Claim 26, wherein said host access security system is
2 a Resource Access Control Facility (RACF) system.

1 Claim 33 (new): A method of enabling a user at a client device to transparently log on to a legacy
2 session with a legacy host application, without requiring change to said legacy host application,
3 comprising steps of:
4 caching a digital certificate associated with said client device, or a user thereof, at a server

Serial No. 09/466,625

-14-

Docket RSW990077

5 to which said digital certificate has been provided for authentication of said client device or said
6 user;

7 initiating, by said server on behalf of said client device, said legacy session with said legacy
8 host application;

9 automatically responding, by said client device, to a log-on request from said legacy host
10 application, where said log-on request is sent by said legacy host application responsive to said
11 initiating step, by sending a log-on message in which placeholder syntax is used in place of a user
12 identifier and password expected by said legacy host application; and

13 before forwarding said sent log-on message from said server to said legacy host
14 application, performing steps of:

15 using said cached digital certificate to obtain, at said server from a host access
16 security system, said expected user identifier and either said expected password or a password
17 substitute therefor which is generated by said host access security system; and

18 replacing said placeholder syntax in said sent log-on message with said obtained
19 user identifier and password or password substitute.